NOTAS DE LA SOLUCIÓN

LA MONITORIZACIÓN DE DOMINIOS SIMILARES PROTEGE SU RED, SUS CLIENTES Y SU MARCA

Detenga de forma proactiva las amenazas de ingeniería social que utilizan dominios similares en ataques dirigidos avanzados con la intención de violar la seguridad de la empresa, comprometer a los clientes o dañar su valiosa marca.

LOS DOMINIOS SIMILARES SON UNA AMENAZA CRECIENTE

Desde ataques a gran escala y de amplio espectro dirigidos a los consumidores hasta spear phishing altamente dirigido, Business Email Compromise (BEC) y otras amenazas empresariales, los dominios similares se han convertido en componentes clave para los adversarios que aspiran a contrarrestar las defensas humanas y técnicas. Pueden suplantar su marca, sus empleados, su cadena de suministro u otros socios de confianza con resultados devastadores.

Aunque se utilizaron por primera vez hace casi dos décadas, los actores maliciosos siguen ideando formas de aplicar los dominios similares en nuevos tipos de ataques. Mediante técnicas de adversario en el medio (AitM), intentan cada vez más engañar a los empleados para que piensen que interactúan con la red real de la empresa durante la autenticación.

Hoy en día, los atacantes utilizan dominios similares en mensajes SMS, llamadas telefónicas, mensajes directos en redes sociales, correos electrónicos y códigos QR. Más recientemente, los atacantes se han centrado en la autenticación multifactorial (MFA) debido a su creciente adopción por parte de todo tipo de usuarios, desde jugadores de videojuegos hasta mercados de divisas digitales, carteras y plataformas de compraventa, como el ataque a Coinbase a principios de 2023. Los dominios similares se han convertido en una parte integral de todas las ciberamenazas importantes.

LOS DOMINIOS SIMILARES SON UNA AMENAZA CRECIENTE

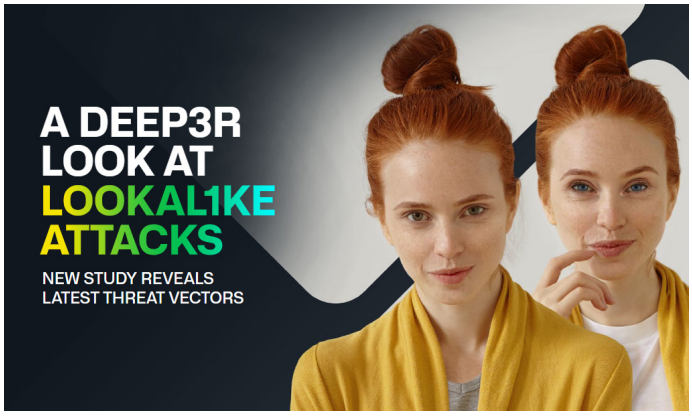

Figura 1: Infoblox Threat Intelligence compartió datos de investigación sorprendentes sobre el creciente riesgo de los dominios similares.

DATOS Y CIFRAS

Otras capacidades avanzadas de seguridad de BloxOne Threat Defense le permiten:

- Se detectaron más de 300.000 dominios similares en poco más de un año
- Los dominios de combosquatting ahora son 100 veces más comunes que los de typosquatting
- Cada día se crean 200.000 dominios nuevos
- En 2023 se utilizaron más de 1.600 dominios para imitar servicios oficiales de MFA
- El 60 % de los dominios de combosquatting están activos durante más de 1.000 días
- Aparte del uso de .com, hoy en día existen otros 1.588 TLD que pueden ser objeto de abuso por parte de los atacantes
- El DNS se utiliza en el 92 % de los ciberataques.

PROTEGER SU MARCA Y A SUS CLIENTES

La defensa contra amenazas de dominios similares a los empresariales requiere un enfoque distinto del utilizado en ataques más dirigidos al consumidor y al mercado masivo. Con la Supervisión de dominios similares de Infoblox, los clientes gestionan su propia lista personalizada de los dominios que les preocupan porque podrían utilizarse en su contra, contra sus empleados o contra sus clientes. A continuación, Infoblox Threat Intelligence supervisa los registradores globales, los ISP, la actividad del DNS real —y mucho más— para identificar posibles dominios similares de alto riesgo en la lista de supervisión del cliente y comenzar la evaluación y el control iniciales. La interfaz de Supervisión de dominios similares ofrece a los clientes visibilidad de los dominios similares identificados y de alto riesgo, así como datos sobre el perfil de riesgo, lo que permite a la organización tomar decisiones con conocimiento de causa, que pueden evitar de forma proactiva una posible violación de la red, ataques a los clientes o daños a la reputación y la marca de la organización.

La Supervisión de dominios similares de Infoblox está disponible por separado y se incluye con la suscripción a la solución DNS Detection and Response (DNSDR) líder del sector de Infoblox, BloxOne Threat Defense Advanced. Estas soluciones conceden a los clientes una licencia para identificar un conjunto inicial de dominios personalizados que se supervisarán en busca de dominios similares de alto riesgo. Los clientes que deseen supervisar más dominios en busca de estos riesgos pueden adquirir licencias adicionales en incrementos de 100 dominios.

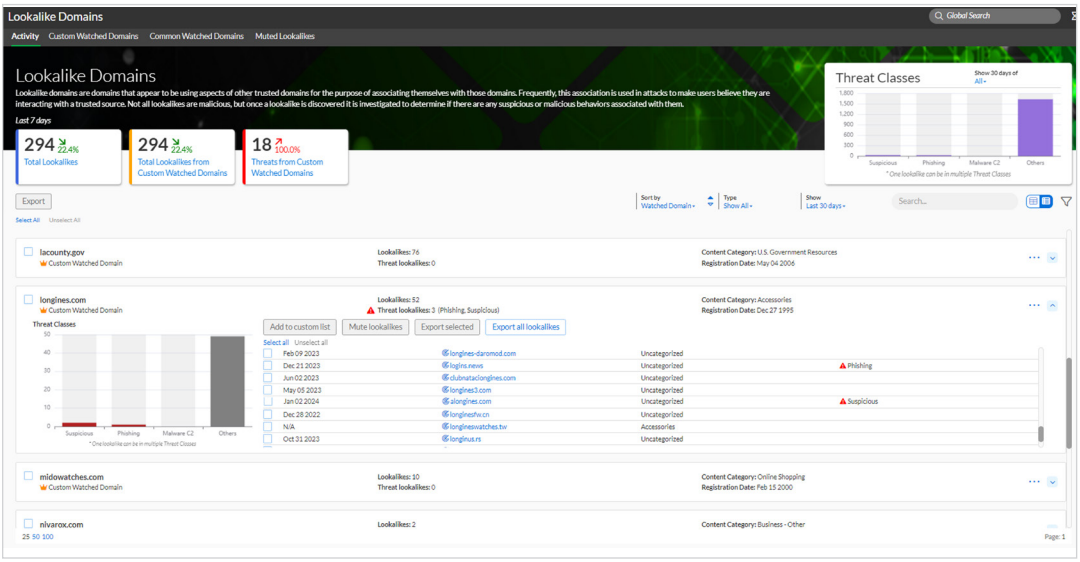

Figura 2: Revise fácilmente los dominios de alto riesgo que se asemejan a otros para comprender los niveles de riesgo que presentan

IMPEDIR QUE EL FRAUDE EN INTERNET ABUSE DE LOS DOMINIOS SIMILARES

Infoblox ofrece «servicios de mitigación de dominios» para ayudar a los clientes a eliminar rápidamente los dominios que suponen un riesgo para su organización o sus clientes. Aplicamos la combinación exclusiva de Infoblox de habilidades de investigación, técnicas automatizadas y relaciones con el sector para resolver problemas con acuerdos de nivel de servicio líderes en el sector que se miden en horas, incluidos el robo de datos, la suplantación de sitios web y otros incidentes cibernéticos, de forma rápida y discreta.

Para obtener más información sobre los servicios de mitigación de dominios de Infoblox, visite https://insights.infoblox.com/es-resources/esr/infoblox-datasheet-infoblox-domain-mitigation-services-es

infoblox.

Infoblox une redes y seguridad para ofrecer un rendimiento y una protección inigualables. Con la confianza de empresas Fortune 100 e innovadores emergentes, proporcionamos visibilidad y control en tiempo real sobre quién y qué se conecta a su red, para que su organización funcione más rápido y detenga antes las amenazas.

Sede corporativa
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054 (EE. UU.)

+1.408.986.4000
www.infoblox.com/es

Versión: 20240125v3